ABSTRACT

In one embodiment, a method for key verification through time varying item presentation based on a key hash result is described. The method comprises generating a key hash result partially based on both a global identifier provided from a source and an estimated current time at that source. After generating the key hash result, a first time-varying item is produced using the key hash result as an index for a table lookup or generated based on certain bit patterns forming the key hash result. Thereafter, the first time-varying item is presented for comparison with a second time-varying item being contemporaneously presented at the source. These computations are repeated, giving the impression of two views or instances of the same time-varying item. An attacker might be able to match one small portion of such a time sequence of presentations, by luck, but not any large portion of the sequence.